FAD

AO 106 (Rev. 7/87) Affidavit for Search Warrant

FILED
08 APR 24 AM 10:28
CLERK, U.S. DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
BY DEPUTY

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

'08 MJ 1255

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

In the Matter of the Search of

(1.) Lexar 2GB USB flash drive (aka "thumb drive")
(2.) SanDisk micro 4GB cruzer USB flash drive (aka "thumb drive")
(3.) Griffin iTalk USB flash drive (aka "thumb drive")

I ALEX MOORE being duly sworn depose and say:

I am a(n) Special Agent, U.S. Department of State, Diplomatic Security Service and have reason to believe
that __ on the person of or X in/on the items known as:

(1.) Lexar 2GB USB flash drive (aka "thumb drive")
(2.) SanDisk micro 4GB cruzer USB flash drive (aka "thumb drive")
(3.) Griffin iTalk USB flash drive (aka "thumb drive")

in the Southern District of California, there is now concealed a certain person or property, namely (describe the person or property to be seized)

for which search is authorized JMA

See Attachment "A" (Description of Items ~~to Be Seized~~)

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

instrumentalities, contraband, fruits and evidence of document fraud, false statements, and illegal use of an official insignia concerning violations of Title 18, United States Code, Section(s) 716, 1001 and 1028. The facts to support a finding of Probable Cause are as follows:

See attached affidavit - continued on the attached sheet and made a part hereof.

Signature of Affiant

Sworn to before me, and subscribed in my presence

San Diego, California at 4/23/08 @ 4:35 p.m.
Date/Time issued

JAN M. ADLER
United States Magistrate Judge
U.S. MAGISTRATE JUDGE
Name and Title of Judicial Officer

Signature of Judicial Officer

R

FAS

ATTACHMENT A – Description of Items ~~to be seized~~: to be seized authorized JMA

Letters, insignia, official documents, legal documents, notarized documents, stamps, seals, banking records, credit reports, credit cards, credit card statements, bills, invoices, documents, letters, telephone records, correspondence or communication, computer software, computer passwords, or other record referencing:

> the acquisition, manufacture, notarization, use, transfer, or distribution of fraudulent identities or fraudulent ambassador or diplomatic identifications, credentials or license plates, and notarization of same referencing James Francis Murphy or James Murphy or James F. Murphy or J. Murphy.

Computerized records or documents pertaining to the acquisition, sale or transfer of embossing machines/presses or document manufacturing devices, including but not limited to computer hardware, computer software and laminating machines.

FM

Affidavit in Support of Search Warrant

I, Alex R. Moore, after being duly sworn, depose as follows:

1. I am a Special Agent with the United States Department of State (hereinafter, "State Department"), Diplomatic Security Service, and have been so employed for 23 years.

2. I have received specialized training in criminal investigative techniques at the Federal Law Enforcement Training Center in Glynco, Georgia and at the Diplomatic Security Training Center in Dunn Loring, Virginia. My career with Diplomatic Security has included assignments to the Washington Field Office and the Office of Passport Fraud Investigations. I have been accredited as a diplomat during my three tours overseas at U.S. Embassies in Australia, Lebanon, and Sri Lanka. Since September 2005, I have been posted to the State Department's Diplomatic Security Service San Diego Resident Office (SDRO). My duties and responsibilities include conducting criminal investigations of individuals and businesses that have violated federal laws, particularly those laws found in Title 18 of the United States Code.

3. During my employment as a Special Agent with the State Department, I have investigated or assisted in the investigation of numerous violations concerning passport and visa fraud offenses, and other associated crimes, to include violations of Title 18, United States Code, Sections 911, 1001, 1028, 1028A, 1542, 1543, 1544, and 1546. My investigations or assistance has resulted in criminal charges having been brought on behalf of the United States for violations of the same.

4. The facts and circumstances of this investigation have been summarized below for the specific purpose of this application. Since this affidavit is submitted for the limited purpose of obtaining a search warrant, I have not set forth each and every known fact pertinent to this investigation and have included primarily those facts that I believe are necessary to establish probable cause to search the property specified herein.

5. In my capacity as a Special Agent, I have been investigating James Francis MURPHY for possible violations of "Unauthorized Possession of Official Insignia," "Making False Statements and Representations," "Using False Documents," and "Possessing False Documents with the Intent to Defraud the United States." Affiant's investigation to date has disclosed that:

   a) On 02/16/08, Diplomatic Security Service Special Agent (SA) Mike Escott was by San Diego Harbor Police (SDHP) that MURPHY had identified himself as a at the San Diego International Airport and attempted to bypass security screening airport, claiming diplomatic immunity. SA Escott responded to the airport and interviewed MURPHY. MURPHY stated to SA Escott that his status as Diplomat/Ambassador afforded him (MURPHY) immunity and requested his diplomatic pouch. MURPHY was shown and subsequently identified the badge credential that he had previously presented to the Transportation Security (TSA) as his official diplomatic credentials issued by the State of California. Based

notified AV JMA

ON AV JMA

FM

SA Escott's experience and training, he determined that the credentials were not authentic diplomatic credentials issued by the United States Department of State.

b) That same day, Affiant reviewed the documents found in MURPHY's possession, which included a wallet-like credential case that contained an official-looking laminated identification card with MURPHY's name, date of birth, photograph, and the title "Diplomatic Agent" (space) "Ambassador." At the top of the card was the heading "State of California" and below that was a reduced image of the official Seal of the State of California. Near the bottom of the identification card was the statement, "DO NOT Delay, Detain, or Arrest for any offense." Also within the credential case was an official-looking law enforcement-type badge containing a gold star, the official California State Seal, the title "Ambassador/Diplomat," and the number 392594.

c) Affiant examined MURPHY's briefcase and noticed that affixed to the bag was a laminated card labeled "Diplomatic Pouch," on one side, and on the other, the following sentences: "This Diplomatic Pouch, containing twelve official Consular documents, is carried by Ambassador James-Francis: Murphy. This correspondence is inviolable. The Diplomatic Pouch shall not be opened, X-rayed, or detained." At the bottom of the card was a reference to the provisions of the Vienna Convention. Inside this bag were miscellaneous papers, a miniature radiation detector/alarm, and a pen-sized plastic instrument containing an unidentified white powder that was later determined to be inert. MURPHY was also carrying a laptop computer, HP Pavilion PP2180, serial #2CD340KDC. This computer was seized and is currently being held by the U.S. State Department Diplomatic Security Service, San Diego Office. In addition, Murphy was carrying three USB flash drives (also known as "thumb drives") in the bag indicated as being a diplomatic pouch. Those were of the following types: (1.) Lexar 2GB thumbdrive; (2.) SanDisk micro 4GB cruzer thumbdrive; and (3.) Griffin iTalk thumbdrive. These three thumbdrives are currently in the custody the Diplomatic Security Service, San Diego Office.

d) On 02/21/2008, Affiant interviewed three TSA officers who were involved in the incident with MURPHY at the San Diego International Airport on 02/16/2008. Officer Mike Capil was on duty at Checkpoint 6 when the TSA ticket checker brought MURPHY to his attention. Officer Capil stated that MURPHY flashed the aforementioned badge, lifted the bag identified by a diplomatic pouch tag, stated he was a diplomat with a diplomatic pouch he "wanted to bring around" the security screening procedure. TSA Supervisor Christine Loftus stated that she was called to Checkpoint 6 and MURPHY identified himself as a diplomat to her. TSA Security Manager Alfredo Ramos was then called to Checkpoint 6 and reviewed the credentials presented by MURPHY. Officer Ramos stated that MURPHY then claimed to be "a diplomatic courier for an ambassador" and pointed to the aforementioned bag marked with a diplomatic pouch tag and said, "this is the bag that cannot go through screening." Officer Ramos asked MURPHY for his diplomatic courier letter and diplomatic passport, and MURPHY responded that he had neither. Officer Ramos asked MURPHY for some other form of identification, and MURPHY responded that he had nothing but the diplomatic credentials.

FAS

e) On 02/22/2008, Affiant obtained federal arrest warrant #08MJ0521, signed by United States Magistrate Judge William McCurine, Jr., against James Francis MURPHY for violations of 18 U.S.C. 1028 (Use of false Identification Document) and 18 U.S.C. 716 (Unauthorized Possession of Official Insignia). On 02/25/2008, Affiant served the warrant and MURPHY was arrested.

f) On 03/04/2008, Affiant, accompanied by DS Special Agent Dan Messelt, visited the MURPHY address at 807 Hymettus Avenue. On the first drive by the residence, Affiant noticed two vehicles in the driveway. The first vehicle, a white Chrysler mini-van, had no license plate. The second vehicle, a red Lexus sedan, had an unfamiliar license plate with a red and blue stripe that did not appear to be standard-issue by a State. Affiant also noticed an unidentified man standing in the garage with the garage door opened. After Affiant and Agent Messelt parked their vehicle and walked to the front of the house, Affiant noticed the license plate had been removed from the Lexus and the garage door was closed. Two fraudulent diplomatic license plates have since been recovered from the Murphy household.

g) On 03/24/2008, Affiant discovered that the diplomat/ambassador badge used by MURPHY at the airport was manufactured by Maxsell Corporation. Maxsell Corporation is located in Florida and operates via an internet website: www.Maxsell.com. According to records provided by Maxsell, two (2) badges were ordered by, and shipped to, James Francis MURPHY. According to the records provided, MURPHY provided two Apostilles to Maxsell in support of his order. One of these Apostilles (both of which were faxed to Maxsell) was the same presented by MURPHY on February 16, 2008, at San Diego International Airport. The second Apostille contained the number 329595, which was imprinted on the ambassador/diplomat badge shipped to MURPHY. Both ambassador/diplomat badges were shipped via UPS. Investigation has revealed that MURPHY paid for these items using his credit card via the internet. This second badge has since been recovered from the Murphy household.

6. Definitions

a) The terms "record," "documents," "invoices," and "correspondence" includes all of described items of evidence in whatever form and by whatever means such records, documents, invoices or correspondence, their drafts, or their modifications may been created or stored, including (but not limited to) any handmade form, (such as writing or drawing, with any implement on any surface, directly or indirectly); any photographic form (such as prints, slides, negatives, videotapes or photocopies); any mechanical form, such as tape recording, cassettes, compact disks, or any electrical, electronic or magnetic storage device (commonly called computer hardware), such floppy diskettes, hard disks, backup tapes, CD-ROMs, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well printouts or readouts from any magnetic storage device.

b) Computer hardware consists of all equipment that can collect, analyze, create, convert, store, conceal or transmit electronic, magnetic optical or similar computer

FAS

impulses or data. Hardware also includes any data processing devices, such as processing units, memory typewriters, self contained "laptop" or "notebook" and personal digital assistants; internal and peripheral storage devices, such as disks, external hard drives, floppy disk drives and diskettes, tape drives and tapes, storage devices, transistor like binary devices and other memory storage devices; peripheral input/output devices, such as keyboards, printers, scanners, plotter, display monitors and optical readers; and related communication devices, such as modems or cables and connections; as well as any devices, mechanisms or parts that be used to restrict access to computer hardware, such as physical keys and locks.

c) Computer software is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical or digital form. It commonly includes programs to run operating systems, applications (like word processing, graphics or spreadsheets), utilities, compilers, interpreters and communications programs.

d) Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or programming code. A password (a string of alphanumeric characters), usually operates as a sort of digital keys to unlock particular data security devices. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or "booby-trap" protected data to make it inaccessible or unstable, as well as reverse the process to restore it.

7. Based upon my personal, law enforcement and investigative experience, Affiant has found that individuals often use computers and related devices for the storage of information related to files (such as correspondence, notes and other documentation) and financial records (such as credit card records and payment receipts). In addition, Affiant has found that individuals often use computers to communicate electronically and purchase items via the internet. Furthermore, based upon my knowledge, experience and training, your affiant knows that searching and seizing information from computer-related implements often require examination by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a) The volume of the evidence. Computer storage devices, such as hard drives, tapes, diskettes, laser disks, CDs, can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

FAS

b) Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. Furthermore, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password protected, or encrypted files. Since computer evidence can be vulnerable to modification or destruction, both from external sources and/or destructive code imbedded in the system as a "booby trap," a controlled environment is essential to its complete and accurate analysis.

c) Furthermore, in my experience, and from my conversations with computer forensic examiners, computer evidence can remain stored on computers for extended periods of time. Even when computer evidence is deleted it may still be recovered from computer hard drives, floppy disks or other computer information storage devices. Computers also create temporary files and store items in temporary locations known as a cache, during normal computer operations. This information can often be recovered by a computer forensic examiner and is likely to have been generated by and remain on any computer used in this scheme.

8. It is Affiant's belief that probable cause exist to believe that documents and items set forth in attachment "B" are concealed within the items set forth in attachment "A," and further, it is Affiant's belief that these documents and items are believed to be evidence and instrumentalities of violations of Title 18, United States Code, Sections 716, 1001, 1028.

Signature of Affiant

Sworn to before me, and subscribed in my presence

San Diego, California at 4/23/08 @ 4:35 p.m.
Date/Time issued

United States Magistrate Judge
Name and Title of Judicial Officer

Signature of Judicial Officer

FAS

ATTACHMENT A – Description of Individual, Premises and Items to be searched:

(1.) Lexar 2GB USB flash drive (aka "thumb drive")
(2.) SanDisk micro 4GB cruzer USB flash drive (aka "thumb drive")
(3.) Griffin iTalk USB flash drive (aka "thumb drive")

for what search is authorized JMA

ATTACHMENT B – Description of Items ~~to be seized~~:

Letters, insignia, official documents, legal documents, notarized documents, stamps, seals, banking records, credit reports, credit cards, credit card statements, bills, invoices, documents, letters, telephone records, correspondence or communication, computer software, computer passwords, or other record referencing:

> the acquisition, manufacture, notarization, use, transfer, or distribution of fraudulent identities or fraudulent ambassador or diplomatic identifications, credentials or license plates, and notarization of same referencing James Francis Murphy or James Murphy or James F. Murphy or J. Murphy.

Computerized records or documents pertaining to the acquisition, sale or transfer of embossing machines/presses or document manufacturing devices, including but not limited to computer hardware, computer software and laminating machines.